



Europäisches Patentamt  
European Patent Office  
Office européen des brevets

Veröffentlichungsnummer:

0 383 985  
A1

12

## EUROPÄISCHE PATENTANMELDUNG

Anmeldenummer: 89103290.6

Int. Cl.<sup>5</sup> H04L 9/00

Anmeldetag: 24.02.89

Veröffentlichungstag der Anmeldung:  
29.08.90 Patentblatt 90/35

Benannte Vertragsstaaten:  
AT BE CH DE ES FR GB IT LI NL SE

Anmelder: Schnorr, Claus Peter, Prof. Dr.  
Frankfurter Strasse 81  
D-6350 Bad Nauheim(DE)

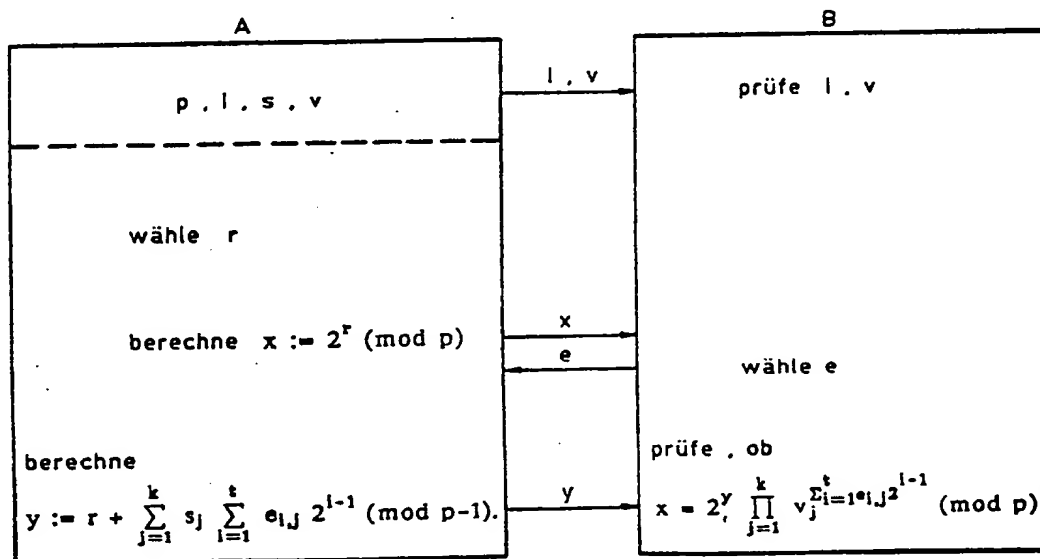
Erfinder: Schnorr, Claus Peter, Prof. Dr.  
Frankfurter Strasse 81  
D-6350 Bad Nauheim(DE)

Vertreter: Fuchs, Franz-Josef, Dr.-Ing. et al  
Postfach 22 13 17  
D-8000 München 22(DE)

Verfahren zur Identifikation von Teilnehmern sowie zur Generierung und Verifikation von elektronischen Unterschriften in einem Datenaustauschsystem.

Bei dem mit Prozessor-Chipkarten arbeitenden Datenaustauschsystem sendet die Chipkarte verschlüsselte Identifikationsdaten  $l, v$  und ausgehend von einem zufälligen diskreten Logarithmus  $r$  einen Exponentialwert  $x = 2^r \pmod{p}$  an den Teilnehmer, der seinerseits eine zufällige Bitfolge  $e$  an die Chipkarte sendet. Die Chipkarte berechnet durch Multiplikation der gespeicherten geheimen Schlüssel  $s$  mit der Bitfolge  $e$  und durch Addition der Zufallszahl  $r$  einen  $y$ -Wert und überträgt diesen  $y$ -Wert an den Teilnehmer, der seinerseits aus  $y, v$  und  $e$  einen  $x$ -Wert errechnet und prüft, ob der errechnete  $x$ -Wert mit dem übermittelten  $x$ -Wert übereinstimmt. Für eine elektronische Unterschrift wird aus einem  $x$ -Wert und der zu unterschreibenden Nachricht  $m$  zunächst ein Hash-Wert  $e$  und anschließend ein  $y$ -Wert aus  $r, s_j$  und  $e$  berechnet. Die Zahlen  $x$  und  $y$  ergeben dann die elektronische Unterschrift zur Nachricht  $m$ .

FIG 1



# Verfahren zur Identifikation von Teilnehmern sowie zur Generierung und Verifikation von elektronischen Unterschriften in einem Datenaustauschsystem

Die Erfindung betrifft Verfahren zur Identifikation von Teilnehmern sowie zur Generierung und Verifikation von elektronischen Unterschriften nach den Merkmalen der Oberbegriffe der Ansprüche 1, 2, 3, 10 und 11.

Wichtige Voraussetzungen für die Datensicherheit in modernen Kommunikationssystemen sind:

- a) Die gegenseitige Identifikation der am System beteiligten Kommunikationspartner
- b) die Authentifikation der übertragenen und gespeicherten Daten
- c) die Verschlüsselung der übertragenen und gespeicherten Daten und
- d) die Prüfung der Urheberschaft der übertragenen Daten.

Ein hohes Maß an Datensicherheit ist bekanntlich nur durch den Einsatz kryptographischer Verfahren zu erreichen, die eine Identifikation und Authentizitätsprüfung von Nachrichten, Teilnehmern und Geräten zweifelsfrei ermöglichen. Unter Kryptographie wird im allgemeinen eine Verschlüsselung der Daten zur Geheimhaltung verstanden. Neben dieser zweifellos wichtigen Kryptofunktion gewinnen aber zunehmend andere Funktionen, insbesondere die Prüfung der Authentizität und Urheberschaft oder die Erzeugung elektronischer Unterschriften an Bedeutung.

Zur Realisierung kryptographischer Funktionen können symmetrische oder asymmetrische Verschlüsselungsalgorithmen verwendet werden. Beim symmetrischen Algorithmus, z.B. dem DES-Algorithmus (Data Encryption Standard) werden zum Ver- und Entschlüsseln gleiche Schlüssel verwendet. Symmetrische Schlüsselsysteme eignen sich vor allem dann, wenn größere Datenmengen mit hoher Geschwindigkeit übertragen werden müssen. Nachteile ergeben sich dagegen durch ein relativ schwieriges Schlüssel-Management, weil Sender und Empfänger den gleichen Schlüssel haben müssen und zur Übertragung des jeweils verwendeten Schlüssels ein sicherer Kanal benötigt wird.

Bei asymmetrischen Schlüsselsystemen werden zum Ver- und Entschlüsseln unterschiedliche Schlüssel verwendet, derart, daß z.B. der Schlüssel zum Verschlüsseln öffentlich und der Schlüssel zum Entschlüsseln geheim ist. Letzterer ist nur dem Empfänger bekannt. Ein unsymmetrisches Schlüsselsystem ist z.B. der nach den Erfindern Rivest, Shamir und Adleman benannte RSA-Algorithmus, der einen vergleichsweise hohen technischen Aufwand und je nach verwendeter Schlüssellänge entsprechend lange Durchlaufzeiten benötigt, aber durch das besondere Schlüsselsystem hohen Sicherheitsanforderungen genügt. Ideal geeignet ist das asymmetrische Schlüsselsystem zum Signieren einer zu übertragenden Nachricht. Die zu unterschreibende Nachricht wird dabei mit dem Geheimschlüssel des Unterschreibenden verschlüsselt und kann von jedem, der den öffentlichen Schlüssel kennt, entschlüsselt werden. Diese "Elektronische Unterschrift" beinhaltet nicht nur das persönliche Merkmal (Besitz des Geheimschlüssels) des Unterschreibenden, sondern bezieht auch den unterschriebenen Text mit ein, mit der Folge, daß jede Änderung des Textes vom Empfänger erkannt wird. Nachricht und Unterschrift sind damit über den Schlüssel-Algorithmus unveränderbar verknüpft.

Der Einsatz moderner kryptographischer Mittel hängt eng mit der Einführung der sogenannten multifunktionalen Prozessor-Chipkarte zusammen. Die Prozessorchipkarte ermöglicht nicht nur vielseitige Anwendungen, sondern ist auch dafür vorgesehen, die notwendigen Sicherheitskomponenten (Geheimschlüssel und Kryptoalgorithmus) aufzunehmen, um eine Identifikation des Benutzers und eine sichere Authentifikation der Karte und der ausgetauschten Nachricht zu gewährleisten.

Die derzeit bekannten Algorithmen für elektronische Unterschriften, insbesondere der RSA-Algorithmus (siehe US-A 4 405 829) und der von A.Fiat und A.Shamir entwickelte Algorithmus (EP A 0 252 499) erfordern entweder einen hohen Speicheraufwand oder benötigen, sofern sie überhaupt im Chip untergebracht werden können, wegen umfangreicher und komplizierter Rechenoperationen, insbesondere Multiplikationen, sehr viel Zeit, so daß sie für den Einsatz in Chipkarten nur bedingt geeignet sind.

Der vorliegenden Erfindung liegt deshalb die Aufgabe zugrunde, Verfahren zur gegenseitigen Identifikation von Teilnehmern eines Datenaustauschsystems und zur Generierung von Unterschriften anzugeben, die bei im wesentlichen gleichen Sicherheitsgarantien aufgrund einfacherer Rechenoperationen im Vergleich zu bekannten kryptographischen Verfahren kürzere Laufzeiten ermöglicht.

Diese Aufgabe wird erfindungsgemäß durch die Merkmale der Ansprüche 1 bzw. 2 und 3 gelöst. Vorteilhafte Ausgestaltungen der Erfindung sind in den übrigen Unteransprüchen angegeben. Dies gilt insbesondere für den Anspruch 4, demzufolge die Verfahren durch in einem Vorprozeß errechnete und zwischengespeicherte diskrete Logarithmen beschleunigt werden können, wobei einmal benutzte Werte in einem Erneuerungsprozeß mit anderen diskreten Logarithmen in zufälliger Weise kombiniert werden. Ein Verfahren zur Verifizierung einer gemäß Anspruch 2 generierten Unterschrift ist in Anspruch 10 angegeben.

Das bei der Erfindung zu lösende Problem besteht in der Schwierigkeit, den diskreten Logarithmus zu berechnen. Auf dieser Grundlage bauen auch andere, bereits bekannte asymmetrische Kryptoverfahren auf: (siehe T. ELGAMAL, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory 31 (1985), 469 - 472; D. CHAUM, J.H. EVERTSE, J. van de GRAAF, J.: "An Improved Protocol for Demonstration Possession of Discrete Logarithms and some Generalizations," Proceedings of Eurocrypt 87, Lecture Notes in Computer Science 304, (1988), 127 - 141; T. BETH: "A Fiat-Shamir-like Authentication Protocol for the ELGAMAL Scheme," Eurocrypt'88 Abstracts p. 41 - 47). Die vorliegende Erfindung hat gegenüber den bekannten Kryptoverfahren den Vorteil, daß die Rechenoperationen in der Chipkarte vergleichsweise einfacher durchgeführt werden können. Dies geschieht insbesondere durch den genannten Vorprozeß. Dieser Vorprozeß kann auch mit den genannten Kryptosystemen von ELGAMAL, CHAUM-EVERTSE-van de GRAAF und BETH kombiniert werden. Darüber hinaus können durch die vorliegende Erfindung besonders kurze Unterschriften erzeugt werden.

Im folgenden werden Einzelheiten der erfindungsgemäßen Verfahren, teilweise anhand der Zeichnung, näher erläutert. In der Zeichnung zeigen

FIG 1 den prinzipiellen Ablauf bei der erfindungsgemäßen Identifizierung eines Teilnehmers,

FIG 2 die erfindungsgemäßen Verfahrensschritte bei der Generierung einer Unterschrift für eine zu übertragende Nachricht,

FIG 3 die Prüfung der gemäß FIG 2 erzeugten Unterschrift,

FIG 4 die erfindungsgemäßen Verfahrensschritte bei der Generierung einer verkürzten Unterschrift,

FIG 5 die Prüfung der gemäß FIG 4 erzeugten verkürzten Unterschrift.

Anhand des in FIG 1 dargestellten Prinzipbildes soll als Beispiel gezeigt werden, wie ein Teilnehmer A, beispielsweise eine diesem Teilnehmer gehörende Chipkarte, gegenüber einem Teilnehmer B, beispielsweise einem Chipkarten-Terminal, seine Identität nachweist. Bei einem mit Chipkarten arbeitenden Datenaustauschsystem werden die jeweils benutzerbezogenen Chipkarten von einem oder gegebenenfalls mehreren Geheimzentren (Regierungsvertretungen, Kreditkartengesellschaften oder dergleichen) ausgegeben, wobei die Ausgabe der Chipkarten erst dann erfolgt, wenn die Identität des jeweiligen Benutzers geprüft worden ist. Das Zentrum bereitet dann für einen qualifizierten Benutzer einen persönlichen Identifikationsstring I vor (Name, Adresse, ID-Nummer, usw.), fügt diesem Identifikationsstring I den benutzerbezogenen öffentlichen Schlüssel zu, der möglicherweise vom Benutzer selbst erzeugt worden ist und veröffentlicht das aus Identifikationsstring I und öffentlichem Schlüssel v gebildete Paar in einer öffentlich zugänglichen Liste. Das Zentrum sieht den geheimen Schlüssel s selbst nicht und kann ihn deshalb auch nicht verraten. Der Identifikationsstring I, die öffentlichen und geheimen Schlüssel v, s sowie eine vereinbarte Primzahl p werden vor der Kartenausgabe in der Chipkarte gespeichert.

Anstelle des Gebrauchs einer öffentlichen Liste kann das Zentrum jedes Paar I, v, unterzeichnen. Diese Unterschrift ist in der Chipkarte gespeichert und kann mit Hilfe des öffentlichen Schlüssels des Zentrums leicht nachgeprüft werden. Nachdem die Chipkarten und/oder die öffentliche Liste ausgegeben sind, ist keine weitere Interaktion mit dem Zentrum notwendig, weder zur Erzeugung noch zur Prüfung von Unterschriften und Identitäten.

Die Identifikation beginnt mit einer sogenannten Initiation. Dabei sendet der Teilnehmer A bzw. die Chipkarte einen Identifikationsstring I und den öffentlichen Schlüssel v an den die Identität verifizierenden Teilnehmer B bzw. an das zugehörige Terminal. Im Unterschied zu bekannten Kryptoverfahren wird der öffentliche Schlüssel im Terminal verifiziert, d.h. das Terminal prüft den Zusammenhang zwischen dem öffentlichen Schlüssel v und dem Identifikationsstring I und kontrolliert auf diese Weise die Unterschrift des Zentrums. Der öffentliche Schlüssel  $v = (v_1 \dots v_k)$  steht im logischen Zusammenhang mit dem geheimen Schlüssel  $s = (s_1 \dots s_k)$  und ist definiert als  $v_j = 2^{-s_j} \pmod{p}$  für  $j = 1, \dots, k$ .

Dabei ist p eine Primzahl, die mindestens 512 Bit lang ist. Sobald der geheime Schlüssel s gewählt ist, kann man den entsprechenden öffentlichen Schlüssel v leicht berechnen. Der umgekehrte Prozeß, den geheimen Schlüssel s aus dem öffentlichen Schlüssel v zu berechnen, ist deshalb nicht durchführbar, weil die Berechnung des diskreten Logarithmus modulo p für derart große Primzahlen p außer Reichweite heutiger Computer und Algorithmen ist. Die Komponente  $s_j$  des geheimen Schlüssels ist der diskrete Logarithmus modulo p von  $v_j^{-1}$ , d.h.

$$s_j = -\log_2 v_j \pmod{p-1} \text{ für } j = 1, \dots, k.$$

Alle diskreten Logarithmen beziehen sich auf die Gruppe  $\mathbb{Z}_p^*$  (die multiplikative Gruppe modulo p) und, sofern nicht anders vermerkt, auf die Basis 2. Weil die Ordnung der Gruppe  $\mathbb{Z}_p^*$  p - 1 ist, nimmt der diskrete Logarithmus die Werte 1, 2, ... p - 1 an.

Anstelle der endlichen Gruppen, die durch Restbildung modulo p entstehen, können auch andere endliche Gruppen zur Bildung des diskreten Logarithmus verwendet werden, wie zum Beispiel der Einheitengruppe

$\mathbb{Z}_n^*$ , der zur Zahl  $n$  primen Restklassen, der Einheitengruppe endlicher Körper, der elliptischen Kurve über einem endlichen Körper, usw.. Zur Übertragung des Verfahrens auf eine beliebige endliche Gruppe ist die Kenntnis der Gruppenordnung nicht erforderlich. Es reicht z.B. aus, mit den diskreten Logarithmen der Größenordnung  $2^{140}$  zu rechnen.

- 5 Nach der Initiierung erfolgt als zweiter Schritt beim Teilnehmer A die Generierung einer Zufallszahl  $r \in (1, \dots, p-1)$ , aus welcher der folgende Exponentialwert  $x := 2^r \pmod{p}$  berechnet wird. Der umgekehrte Rechenprozeß, d.h. aus dem  $x$ -Wert die Zufallszahl  $r$  zu berechnen, ist sehr schwierig, so fern  $p$  hinreichend groß ist. Der Teilnehmer B hat deshalb praktisch keine Möglichkeit, die Zufallszahl  $r$  in der ihm zur Verfügung stehenden Zeit auszuforschen. Dieser beim Teilnehmer A berechnete  $x$ -Wert wird an den Teilnehmer B, d.h. an das Terminal übertragen. Die Zufallszahl  $r$  ist, wie der bereits vorher erwähnte Geheimschlüssel  $s_j$ , ein diskreter Logarithmus. Daraus folgt, daß auf der Chipkarten-Seite mit diskreten Logarithmen, auf der Gegenseite d.h. im Terminal des Teilnehmers B mit dem jeweiligen Exponentialwert gerechnet wird.

- 15 Die Generierung der Zufallszahl  $r$  und der daraus abgeleiteten Exponentialfunktion  $x := 2^r \pmod{p}$  kann nun in vorteilhafter Weise durch einen Vorprozeß beschleunigt werden, der in der Chipkarte einen Vorrat von mehreren Paaren, bestehend aus je einer Zufallszahl  $r$  und dem dazugehörigen  $x$ -Wert, bereitstellt und erneuert. Dieser Vorrat kann in der Chipkarte selbst angelegt oder von außen in die Chipkarte geladen werden. Bei einem initiierten Identifikations-Prozeß kann deshalb sofort auf eines dieser Paare zugegriffen werden, so daß der jeweilige  $x$ -Wert unverzüglich an den Teilnehmer B übertragen werden kann.

- Im nächsten Schritt sendet nun der Teilnehmer B eine zufällige Bitfolge  $e = (e_{1,1}, \dots, e_{t,k}) \in \{0,1\}^{kt}$  an den Teilnehmer A bzw. an die Chipkarte.

Nach Empfang der zufälligen Bitfolge  $e$  sendet die Chipkarte eine von den Bits der zufälligen Bitfolge  $e$  abhängige Linearkombination der bei ihr gespeicherten geheimen Schlüssel  $s_j$ , addiert dazu die aktuelle Zufallszahl  $r$  und sendet den so gebildeten Zahlenwert  $y$

$$y := r + \sum_{j=1}^k s_j \sum_{i=1}^t e_{i,j} 2^{i-1} \pmod{p-1}$$

an den Teilnehmer B.

Der Teilnehmer B prüft nun nach, ob der an ihn gesendete  $y$ -Wert auch die richtige Antwort auf die gestellte Frage ist, welche nämlich der Teilnehmer A durch Senden der Zufallsbitfolge  $e$  gestellt hat. Bei dieser Prüfung berechnet der Teilnehmer B den rechten Teil der folgenden Gleichung

$$x = 2^y \prod_{j=1}^k v_j \sum_{i=1}^t e_{i,j} 2^{i-1} \pmod{p}$$

und stellt anhand eines Vergleichs fest, ob der errechnete Zahlenwert  $x$  mit dem bereits vorher vom Teilnehmer A erhaltenen  $x$ -Wert übereinstimmt. Dieser beim Teilnehmer B durchzuführende Rechenprozeß ist zwar relativ aufwendig, aber wegen der im Terminal in aller Regel ausreichend vorhandenen Rechnerleistung in relativ kurzer Zeit durchführbar. Damit ist die Identifikationsprüfung abgeschlossen, so daß, sofern beim Teilnehmer B eine Übereinstimmung der beiden  $x$ -Werte festgestellt worden ist, seitens des Teilnehmers A weitere Maßnahmen eingeleitet werden können.

Die beschriebene Identifikation des Teilnehmers A kann durch Einbeziehen einer Nachricht  $m$  zu einer elektronisch erzeugten Unterschrift des Teilnehmers A unter die Nachricht  $m$  erweitert werden. Diese elektronische Unterschrift gestattet es, dem Teilnehmer B die Identität von A gegenüber einem Dritten, z.B. einem Richter nachzuweisen. Sie gestattet darüber hinaus den Nachweis, daß der Teilnehmer A zweifelsfrei die Nachricht  $m$  unterschrieben hat. Um unter Benutzung der beim Teilnehmer A, d.h. in der Chipkarte

gespeicherten geheimen Schlüssel  $s_j$  eine Nachricht  $m$  zu unterzeichnen, sind folgende Schritte auszuführen (siehe FIG 2):

1. Der Teilnehmer A wählt wieder eine Zufallszahl  $r$  und berechnet daraus, wie bereits im Zusammenhang mit der Identifikationsprüfung beschrieben, einen  $x$ -Wert gemäß der Beziehung

$$x := 2^r \pmod{p}$$

Auch hier besteht selbstverständlich die Möglichkeit, auf den gespeicherten Vorrat zurückzugreifen und die Zufallszahlen  $r$  und den zugehörigen  $x$ -Wert unmittelbar abzurufen.

2. Der Teilnehmer A bildet nun einen Hashwert  $e$  aus der Nachricht  $m$  und dem ermittelten bzw. aus dem Vorrat entnommenen  $x$ -Wert gemäß der Beziehung

$$e := h(x, m) \in \{0, 1\}^{kt}$$

Dabei ist  $h$  eine öffentlich bekannte Hashfunktion mit Werten in  $\{0, 1\}^{kt}$ .

3. Schließlich berechnet der Teilnehmer A aus den Komponenten: Geheimer Schlüssel  $s_j$ , Zufallsbitfolge bzw. Hashwert  $e$  und der Zufallszahl  $r$  einen  $y$ -Wert gemäß der Beziehung

$$y := r + \sum_{j=1}^k s_j \sum_{i=1}^t e_{i,j} 2^{i-1} \pmod{p-1}$$

Das Zahlenpaar  $x, y$  ergibt sodann die sogenannte elektronische Unterschrift zur Nachricht  $m$ . Die beiden Sicherheitszahlen  $k$  und  $t$  liegen vorzugsweise im Bereich zwischen 1 und 20. Sie ergeben ein Sicherheitsniveau  $2^{kt}$ , das heißt wenigstens  $2^{kt}$  Multiplikationen (modulo  $p$ ) sind zur Fälschung der Unterschrift bzw. der Identität notwendig. Beispielsweise ergibt  $k = 4$  und  $t = 18$  ein für Unterschriften hinreichendes Sicherheitsniveau  $2^{72}$ .

Ausgehend von dieser durch die Zahlen  $x$  und  $y$  gebildeten Unterschrift, wobei beide Zahlen mindestens 512 Bit lang sind, ergeben sich verschiedene Möglichkeiten der Unterschriftenverkürzung. Eine der Möglichkeiten sieht vor, die Zahl  $x$  durch den Hashwert  $e = h(x, m)$  zu ersetzen, der nur 72 Bit lang ist. Die Unterschrift besteht dann nur noch aus  $y$  und  $e$  (siehe FIG 4). Ein nächster Schritt besteht darin, die Zahlen  $y, r, s_j$  nicht mehr in der Größe des Moduls  $p$  zu nehmen, sondern für  $y, r, s_j$  nur noch kleine Zahlen zu verwenden, die aber mindestens 140 Bit lang sind. Eine besonders einfache Möglichkeit, kurze Unterschriften zu erzielen, besteht darin, daß man den Primzahl-Modulus  $p$  so wählt, daß eine zweite Primzahl  $q$  den Wert  $(p-1)$  teilt, wobei  $q = 140$  Bit lang ist. Man ersetzt dann die Basis 2 durch eine Zahl  $\alpha$ , so daß

$\alpha^q = 1 \pmod{p}, \alpha \neq 1 \pmod{p}$  ist. Daraus folgt, daß alle diskreten Logarithmen modulo  $q$  berechnet werden können, d.h. man berechnet Logarithmen zu der gewählten Zahl  $\alpha$ , wobei dann alle Logarithmen im Bereich von 1 bis  $q$  liegen. Dies hat den Vorteil, daß sich für den  $y$ -Wert der Unterschrift eine Zahl ergibt, die kleiner als  $q$  ist. Ausgehend von einer Zufallszahl  $r$

$r \in \{1, \dots, q-1\}$ ,  
dem daraus errechneten  
 $x := \alpha^r \pmod{p}$   
sowie der zufälligen Bitfolge  
 $e := h(x, m) \in \{0, 1\}^{kt}$   
und der daraus errechneten Zahl  $y$

$$y := r + \sum_{j=1}^k s_j \sum_{i=1}^t e_{i,j} 2^{i-1} \pmod{q}$$

ergibt sich für die nun aus den Zahlen  $y$  und  $e$  gebildete Unterschrift mit  $y = 140$  Bits und  $e = 72$  Bits insgesamt eine Länge von 212 Bits. Eine derart verkürzte Unterschrift hat das Sicherheitsniveau  $2^{72}$  d.h. etwa  $2^{72}$  Multiplikationen modulo  $p$  sind erforderlich, um eine Unterschrift zu fälschen.

Zur Verifikation einer aus den Zahlen  $x, y$  bestehenden Unterschrift sind beim Teilnehmer B, d.h. im Terminal folgende Schritte vorgesehen. Zunächst wird, wie FIG 3 zeigt,

$$e := h(x, m) \in \{0, 1\}^{kt}$$

berechnet und dann der Gleichheitstest durchgeführt, derart, daß der gemäß der Beziehung

$$\bar{x} = 2^y \prod_{j=1}^k v_j^{\sum_{i=1}^t e_{i,j} 2^{i-1}} \pmod{p}$$

errechnete  $\bar{x}$ -Wert mit dem x-Wert der Unterschrift verglichen wird.

Bei verkürzten Unterschriften, bei denen x durch e ersetzt wird, erfolgt die Verifikation gemäß FIG 5 in der Weise, daß man zunächst

$$\bar{x} = 2^y \prod_{j=1}^k v_j^{\sum_{i=1}^t e_{i,j} 2^{i-1}} \pmod{p}$$

berechnet und dann prüft, ob die Zahl  $\bar{x}$  den richtigen e-Wert liefert. Letzteres erfolgt dadurch, daß man prüft, ob der Hash-Wert  $h(\bar{x}, m)$  mit dem Wert e übereinstimmt.

Sowohl beim Identifikations- als auch beim Unterschriftenprotokoll sind in der Chipkarte nur relativ geringe Rechenleistungen zu erbringen. Bei der Berechnung der Zahl y sind zwar die geheimen Schlüssel  $s_i$  noch mit relativ kleinen Zahlen zu multiplizieren, diese Multiplikation kann aber in einfache Additionen und Verschiebevorgänge, sogenannte Shifts, aufgelöst werden, wobei das Produkt aus  $s_i$  und  $e_{ij}$  nur um  $i-1$  Positionen nach links geschiftet werden muß. Zu diesem Zwischenergebnis ist schließlich noch die Zufallszahl r durch Addition anzufügen.

Die Berechnung der Zahl

$$x: = 2^r \pmod{p}$$

ist zwar auch aufwendig, kann aber durch den bereits erwähnten Vorprozess vom Zeitaufwand her praktisch vernachlässigt werden, wenn für einige Zufallszahlen entsprechende x-Werte vorausberechnet und mehrere Paare, bestehend aus r- und x-Werten, als Vorrat abgespeichert werden.

Um zu verhindern, daß bei einer begrenzten Anzahl von Paaren in regelmäßigen Abständen immer wieder die gleichen Zahlenpaare verwendet werden, findet eine Erneuerung insofern statt, als jedes Paar nach der Benutzung anschließend mit anderen, gegebenenfalls allen Paaren des Vorrats kombiniert wird und zwar wieder auf zufällige Weise. Dies hat zur Folge, daß der Vorrat nach und nach immer wieder erneuert und verändert wird.

Als Beispiel für einen derartigen Erneuerungsprozeß sei angenommen, daß ein Vorrat von  $\bar{k}$  Zahlenpaaren  $(r_i, x_i)$  für  $i = 1, \dots, \bar{k}$  vorliegt. Um das Paar  $(r, x)$  zu erneuern, wählt man zum Beispiel zufällige Indizes  $a(1), \dots, a(\bar{t}-1) \in \{1, \dots, \bar{k}\}$ , sowie ein gerade erneuertes Paar  $(r_\mu, x_\mu)$  und berechnet mit  $a(\bar{t}) = \mu$  das neue Paar  $(r_\nu, x_\nu)$  nach der Vorschrift

$$r_\nu^{\text{neu}} := r_\nu^{\text{alt}} + \sum_{i=1}^{\bar{t}} r_{a(i)} \pmod{p-1}$$

$$x_\nu^{\text{neu}} := x_\nu^{\text{alt}} \cdot \prod_{i=1}^{\bar{t}} x_{a(i)} \pmod{p}$$

Für das neue Paar  $(r_\nu, x_\nu)$  gilt wieder die Beziehung  $x = 2^r \pmod{p}$ . Die neue Zahl r kann man mit  $\bar{t}$  Additionen, die neue Zahl  $x_\nu$  mit  $\bar{t}$  Multiplikationen berechnen. Eine andere Erneuerung des Paares  $(r_\nu, x_\nu)$  ist möglich nach der Vorschrift

$$r_v^{\text{neu}} := r_v^{\text{alt}} + \sum_{i=1}^{\bar{t}} r_{a(i)} 2^i \pmod{p-1}$$

$$x_v^{\text{neu}} := x_v^{\text{alt}} \cdot \prod_{i=1}^{\bar{t}} x_{a(i)} 2^i \pmod{p}.$$

- Die Berechnung des neuen Wertes  $r$  geht hier in  $\bar{t}$  Additionen und  $\bar{t}$  Shifts. Die neue Zahl  $x_v$  kann man mit  $2 \bar{t}$  Multiplikationen berechnen. Hierzu führt man beginnend mit  $z = 1$  die Schritte  
 $z := z x_{a(i)} \pmod{p}$ ,  $z := z^2 \pmod{p}$ ,  
 mit von  $\bar{t}$  nach 1 absteigendem Index  $i$  durch.  
 Den neuen Wert  $x_v$  erhält man als Produkt des alten Wertes mit der zuletzt berechneten Zahl  $z$ , also nach der Vorschrift

$$x_v^{\text{neu}} := x_v^{\text{alt}} z \pmod{p}.$$

- Bei dieser Erneuerung hat die Wahl  $a(\bar{t}) = \mu$  zur Folge, daß eine gerade erneuerte Zahl  $r_\mu$  mit der höchsten  $2^{\bar{t}}$ -Potenz multipliziert wird. Dies führt zu einer besonders effektiven Erneuerung des Vorrats.
- Selbstverständlich kann man diese Erneuerungsprozesse für das Paar  $(r_v, x_v)$  kombinieren und variieren. Es kommt nur darauf an, daß die Erneuerung möglichst schnell geht und aus den geleisteten Unterschriften nicht nachvollziehbar ist. Man benutzt also zweckmäßig eine kleine Zahl  $\bar{t}$ ; die Erneuerung bleibt unausforschbar, wenn der Vorrat an Zahlenpaaren - also die Zahl  $\bar{k}$  - hinreichend groß ist. Es ist vorteilhaft, die Schlüsselpaare  $s_i, v_i$  bei der Erneuerung mit zu benutzen; man kann zum Beispiel für ein Paar  $(r_{a(i)}, x_{a(i)})$  ein Schlüsselpaar  $(s_i, v_i)$  wählen. Bei  $\bar{t} = 6$  und  $\bar{k} = 10$  braucht die Erneuerung eines Schlüsselpaares nur 6 bzw. 12 Multiplikationen, die mehr oder weniger nebenbei durchgeführt werden können, z.B. dann, wenn im Terminal andere Rechenoperationen auszuführen sind.
- Die vielfältigen Möglichkeiten, die Zahlenpaare  $(r_v, x_v)$  zu erneuern, können in jeder Chipkarte anders genutzt werden. Zum Beispiel können die Indizes  $a(1), \dots, a(\bar{t}-1)$  und die Kombinationen der Schlüsselpaare des Vorrats in jeder Chipkarte anders gebildet werden. Auf diese Weise wird ein Ausforschen des Erneuerungsprozesses praktisch unmöglich.
- Im Falle der verkürzten Unterschrift müssen die Zufallszahlen  $r_i$  klein sein, damit auch der  $y$ -Teil der Unterschrift klein bleibt. Dies erreicht man einfach dadurch, daß man für die diskreten Logarithmen eine Basis  $\alpha$  wählt, für die es eine 140 Bit lange Primzahl  $q$  gibt, so daß  $\alpha^q = 1 \pmod{p}$ . Bei der Erneuerung der Zufallszahlen  $r_i$  wird dann natürlich modulo  $q$  gerechnet, d.h. es wird der Modul  $p-1$  durch den Modul  $q$  ersetzt.

## Ansprüche

- Verfahren zur gegenseitigen Identifikation von Teilnehmern in einem mit Prozessor-Chipkarten arbeitenden Datenaustauschsystem, unter Verwendung von in einem Zentrum jeweils mit teilnehmerbezogenen öffentlichen Schlüsseln verschlüsselten und in der jeweiligen Chipkarte gespeicherten Identifikationsdaten und mit diesen öffentlichen Schlüsseln in logischem Zusammenhang stehenden Geheimschlüsseln, bei dem wechselseitig zwischen den Teilnehmern zufallszahlenabhängige Prüfdaten ausgetauscht werden, **gekennzeichnet durch folgende Schritte:**
  - Die Chipkarte sendet die verschlüsselten Identifikationsdaten  $(l, v)$ , gegebenenfalls zusammen mit einer Unterschrift des Zentrums an den mit der Chipkarte in einen Informationsaustausch eintretenden Teilnehmer, der die Korrektheit der verschlüsselten Identifikationsdaten  $(l, v)$  anhand einer öffentlichen

Liste oder der Unterschrift des Zentrums prüft,

b) die Chipkarte bildet, ausgehend von einem zufälligen diskreten Logarithmus  $r$  ( $1, \dots, p-1$ ), wobei  $p$  ein vereinbarter Primzahl-Modulus ist, einen  $x$ -Wert gemäß der Vorschrift

$$x := 2^r \pmod{p}$$

5 und sendet diesen  $x$ -Wert an den Teilnehmer

c) der Teilnehmer sendet eine zufällige Bitfolge

$$e = (e_{1,1}, \dots, e_{t,k}) \in \{0,1\}^{kt}$$

an die Chipkarte

d) die Chipkarte berechnet durch Multiplikation der gespeicherten, ebenfalls einen diskreten Logarithmus darstellenden geheimen Schlüssel  $s_j$  mit einer aus den Bits der vom Teilnehmer zur Chipkarte übertragenen zufälligen Bitfolge  $e$  gebildeten Dualzahl und durch Addition der dem vorher übertragenen  $x$ -Wert zugeordneten Zufallszahl  $r$  eine Zahl  $y$  gemäß der Vorschrift

$$15 \quad y := r + \sum_{j=1}^k s_j \sum_{i=1}^t e_{i,j} 2^{i-1} \pmod{p-1}$$

20 und überträgt diese Zahl  $y$  zum Teilnehmer

e) der Teilnehmer berechnet anhand der ihm übertragenen Zahl  $y$  eine Zahl  $x$  nach der Vorschrift

$$25 \quad x = 2^y \prod_{j=1}^k v_j \sum_{i=1}^t e_{i,j} 2^{i-1} \pmod{p}$$

und prüft die Identität des Chipkarten-Benutzers anhand eines Vergleichs zwischen der errechneten Zahl  $x$  und dem ihm vorher übermittelten  $x$ -Wert.

2. Verfahren zur Erzeugung von Unterschriften für eine zu übertragende Nachricht in einem mit Prozessor-Chipkarten arbeitenden Datenaustauschsystem nach Anspruch 1,

**gekennzeichnet durch** folgende Schritte:

a) Die Chipkarte berechnet aus einer in der Chipkarte erzeugten, im Bereich zwischen 1 und dem Primzahl-Modulus ( $p-1$ ) liegenden Zufallszahl  $r$  einen  $x$ -Wert gemäß der Vorschrift

$$35 \quad x := 2^r \pmod{p}$$

b) die Chipkarte berechnet als Funktion des  $x$ -Wertes, der Nachricht  $m$  und einer vereinbarten Hashfunktion  $h$  eine zufällige Bitfolge gemäß der Vorschrift  $e := h(x, m) \in \{0,1\}^{kt}$

c) die Chipkarte berechnet aus der Zufallszahl  $r$ , den in der Chipkarte gespeicherten Geheimschlüsseln  $s_j$  und der zufälligen Bitfolge  $e$  einen  $y$ -Wert gemäß der Vorschrift

$$45 \quad y := r + \sum_{j=1}^k s_j \sum_{i=1}^t e_{i,j} 2^{i-1} \pmod{p-1}$$

d) die Chipkarte sendet die Nachricht  $m$  und die aus den Werten  $x$  und  $y$  gebildete Unterschrift an den mit ihr im Nachrichtenaustausch stehenden Teilnehmer.

3. Verfahren zur Erzeugung einer verkürzten Unterschrift für eine zu übertragende Nachricht in einem mit Prozessor-Chipkarten arbeitenden Datenaustauschsystem, nach Anspruch 1,

**gekennzeichnet durch** folgende Schritte:

a) Die Chipkarte berechnet aus einer in der Chipkarte erzeugten, im Bereich zwischen 1 und dem Primzahl-Modulus ( $p-1$ ) liegenden Zufallszahl  $r$  einen  $x$ -Wert nach der Vorschrift

$$55 \quad x := 2^r \pmod{p}$$

b) die Chipkarte berechnet als Funktion vom  $x$ -Wert und der Nachricht  $m$  eine zufällige Bitfolge  $e$  gemäß der Vorschrift

$$e := h(x, m) \in \{0,1\}^{kt}$$



c) die Chipkarte berechnet aus der Zufallszahl  $r$ , aus den geheimen Schlüsseln  $s_j$  und aus der Zufallsbitfolge  $e$  einen  $y$ -Wert gemäß der Vorschrift

$$y := r + \sum_{j=1}^k s_j \sum_{i=1}^t e_{i,j} 2^{i-1} \pmod{p-1}$$

d) die Chipkarte sendet die Nachricht  $m$  und die aus den Werten  $e$  und  $y$  gebildete Unterschrift an den mit ihr im Nachrichtenaustausch stehenden Teilnehmer.

4. Verfahren nach einem der vorhergehenden Ansprüche,

**dadurch gekennzeichnet**, daß in der Chipkarte mehrere Zufallszahlen  $r$  und jeweils zugehörige in einem Vorprozeß berechnete  $x$ -Werte paarweise abgespeichert werden, daß das bei einer Identifikations- und/oder Unterschriften-Prozedur verwendete Paar  $(r, x)$  in der Weise verändert wird, daß eine Zufallszahl  $r$  nach Benutzung mit einer zufälligen Auswahl der übrigen gespeicherten Zufallszahlen kombiniert wird und daß zur erneuerten Zufallszahl der zugehörige  $x$ -Wert berechnet und zusammen mit der erneuerten Zufallszahl  $r$  als erneuertes Paar abgespeichert und/oder benutzt wird.

5. Verfahren nach Anspruch 4,

**dadurch gekennzeichnet**, daß in der Chipkarte mehrere Zufallszahlen  $r_1, \dots, r_k$  und ihre zugehörigen  $x$ -Werte,  $x_v = 2^v \pmod{p}$  abgespeichert werden und daß das bei einer Identifikations- und/oder Unterschriften-Prozedur verwendete Paar  $(r, x)$  durch eine zufällige Auswahl  $(r_{a(i)}, x_{a(i)})$  für  $i = 1, \dots, \bar{t}$  der Paare wie folgt erneuert wird

$$r_v^{\text{neu}} := r_v^{\text{alt}} + \sum_{i=1}^{\bar{t}} r_{a(i)} 2^i \pmod{p-1}$$

$$x_v^{\text{neu}} := x_v^{\text{alt}} \cdot \prod_{i=1}^{\bar{t}} x_{a(i)} 2^i \pmod{p}$$

6. Verfahren nach einem der vorhergehenden Ansprüche,

**gekennzeichnet durch** eine derartige Wahl des Primzahl-Modulus  $p$ , daß  $(p-1)$  durch eine Primzahl  $q$  teilbar ist und durch eine derartige Wahl der Basis  $\alpha$  des diskreten Logarithmus, daß

$$\alpha^q = 1 \pmod{p}, \alpha \neq 1 \pmod{p}$$

ist, daß die diskreten Logarithmen  $y, r, s_j$  modulo  $q$  berechnet werden und daß die Schlüsselkomponenten  $s_j$  und  $v_j$  in der Beziehung  $v_j = \alpha^{s_j} \pmod{p}$  stehen.

7. Verfahren nach einem der vorhergehenden Ansprüche,

**gekennzeichnet durch** eine derartige Wahl der geheimen Schlüssel ( $s_j$ ) und der Zufallszahlen ( $r$ ), daß die Bitlängen der Zahlen  $s_j, r$  und  $y$  kürzer als die volle Länge des Primzahl-Modulus  $p$  sind.

8. Verfahren nach einem der vorhergehenden Ansprüche,

**dadurch gekennzeichnet**, daß anstelle der endlichen Gruppen, die durch Restklassenbildung modulo  $p$  entstehen, andere endliche Gruppen zur Bildung des diskreten Logarithmus verwendet werden.

9. Verfahren nach Anspruch 8,

**dadurch gekennzeichnet**, daß als endliche Gruppe eine Einheitengruppe  $\mathbb{Z}\mathbb{Z}_n^*$ , der zur Zahl  $n$  primen Restklassen, eine Einheitengruppe eines endlichen Körpers, eine elliptische Kurve über einem endlichen Körper oder dergleichen vorgesehen sind.

10. Verfahren zur Verifikation einer nach dem Verfahren gemäß Anspruch 2 erzeugten Unterschrift  $(x, y)$  beim die unterschriebene Nachricht  $m$  empfangenen Teilnehmer,

**gekennzeichnet durch** folgende Schritte:

a) Aus der Nachricht  $m$  und dem  $x$ -Wert der Unterschrift wird eine zufällige Bitfolge  $e$  gemäß der

Vorschrift berechnet

$e := h(x, m) \in \{0, 1\}^{kt}$

b) aus der zufälligen Bitfolge  $e$ , dem öffentlichen Schlüssel  $v$  und dem  $y$ -Wert der Unterschrift wird ein  $x$ -Wert gemäß der Vorschrift

$$\bar{x} = 2^y \prod_{j=1}^k v_j^{\sum_{i=1}^t e_{i,j} 2^{i-1}} \pmod{p}$$

berechnet und geprüft, ob der berechnete  $\bar{x}$  Wert mit dem  $x$ -Wert der Unterschrift übereinstimmt.

11. Verfahren zur Verifikation einer nach dem Verfahren gemäß Anspruch 3 erzeugten, verkürzten Unterschrift beim die unterschriebene Nachricht  $m$  empfangenen Teilnehmer,

**gekennzeichnet durch** folgende Schritte:

a) Aus der übertragenen Nachricht  $m$  und der Unterschrift  $(e, y)$  wird eine Zahl  $\bar{x}$  gemäß der Vorschrift berechnet

$$\bar{x} = 2^y \prod_{j=1}^k v_j^{\sum_{i=1}^t e_{i,j} 2^{i-1}} \pmod{p}$$

b) Es wird geprüft, ob der  $e$ -Wert der Unterschrift übereinstimmend mit  $h(\bar{x}, m)$ .

FIG 1

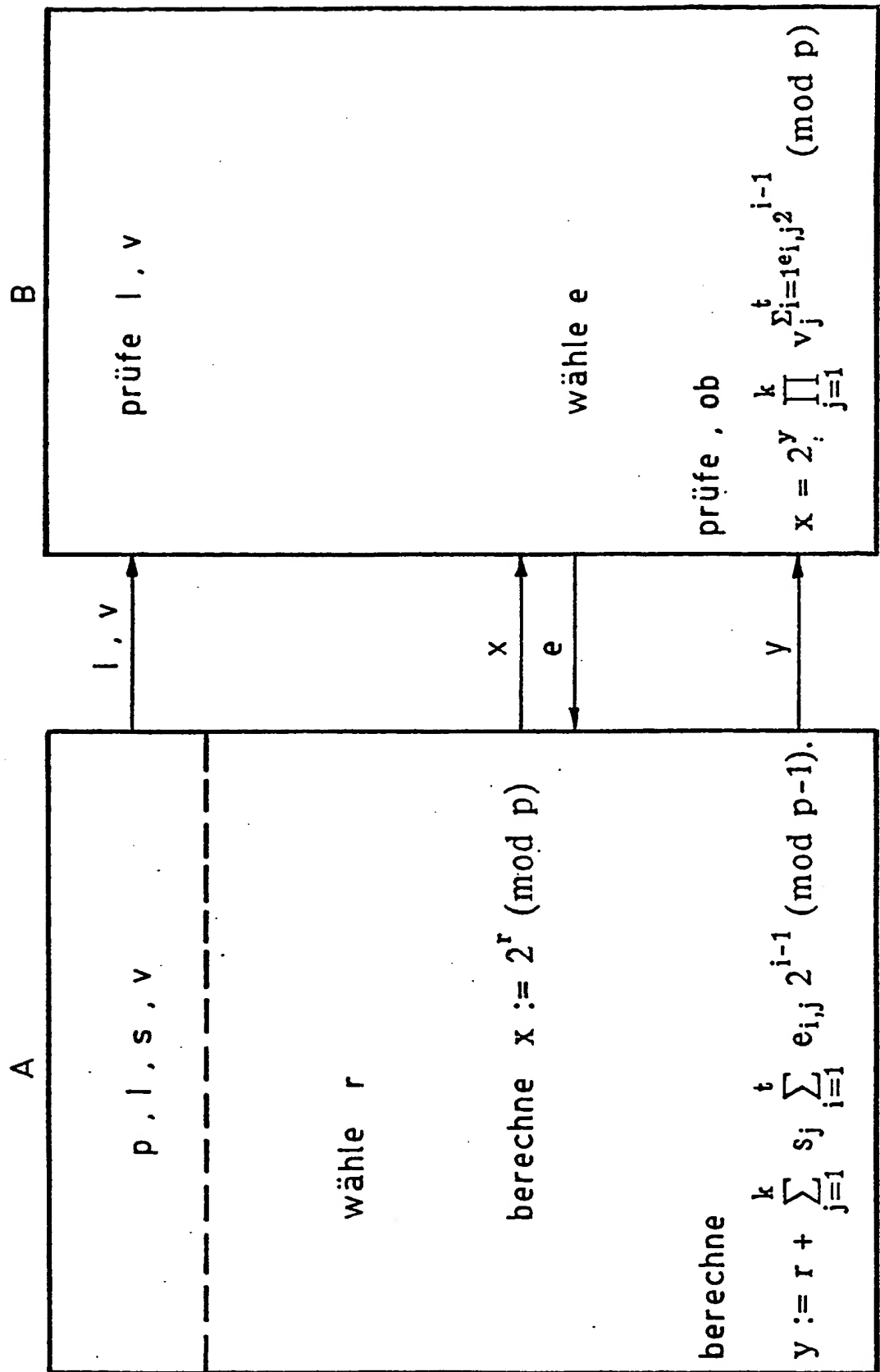


FIG 2

A

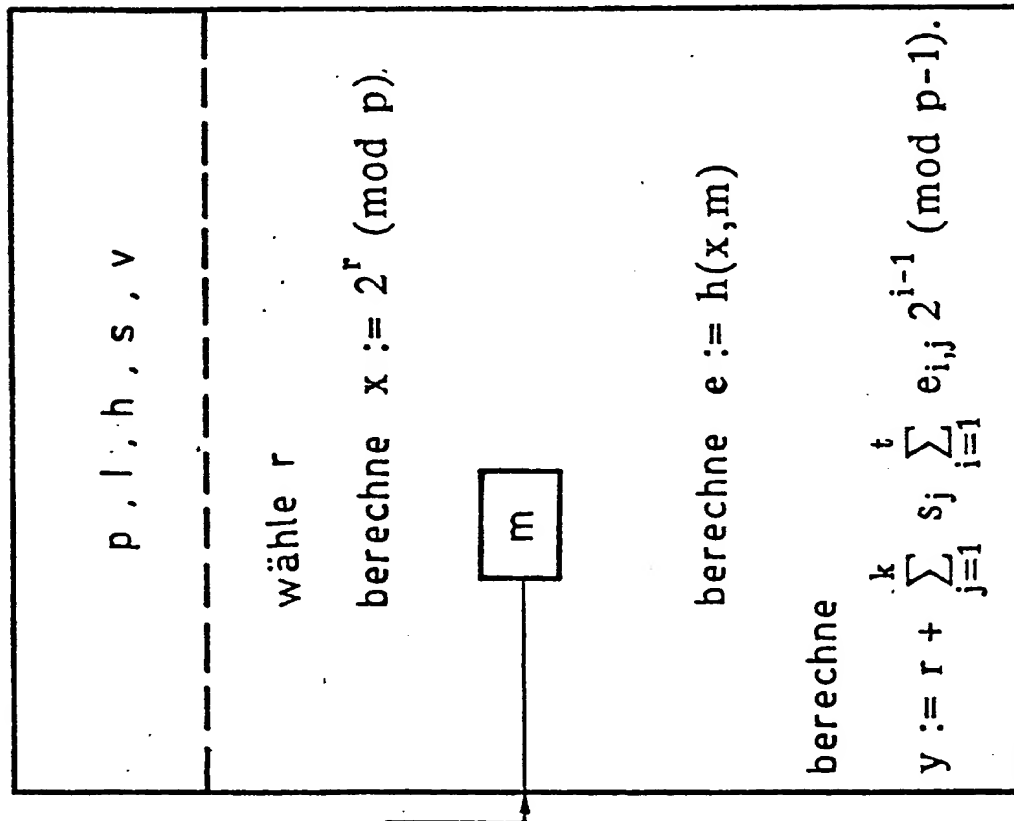


FIG 4

B

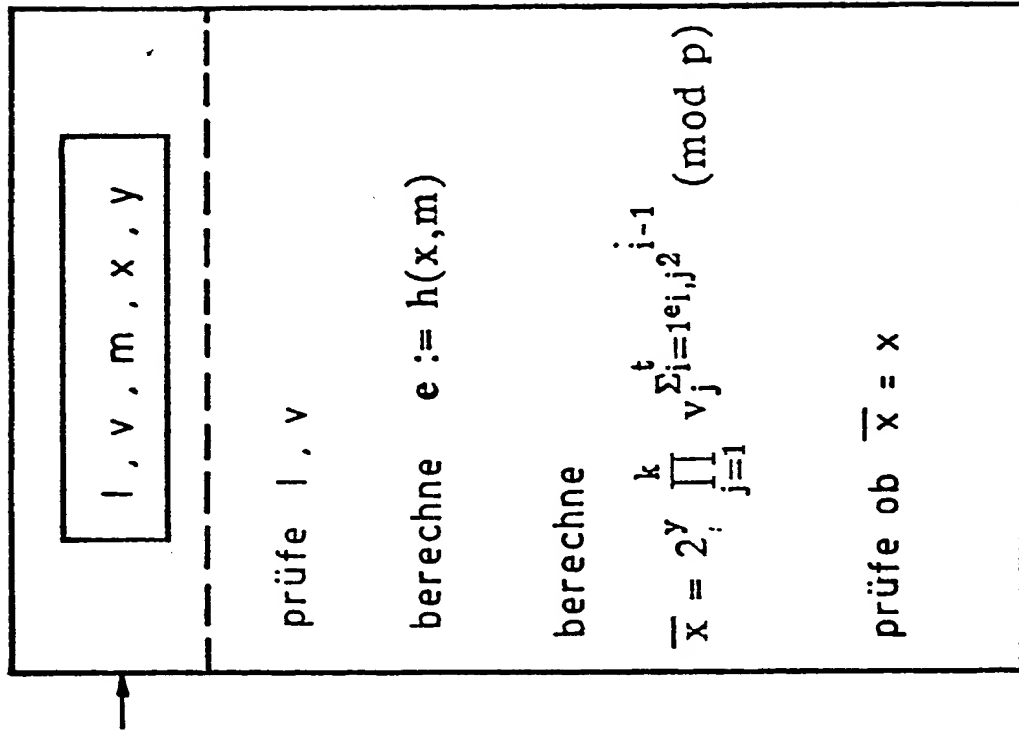


FIG 3

A

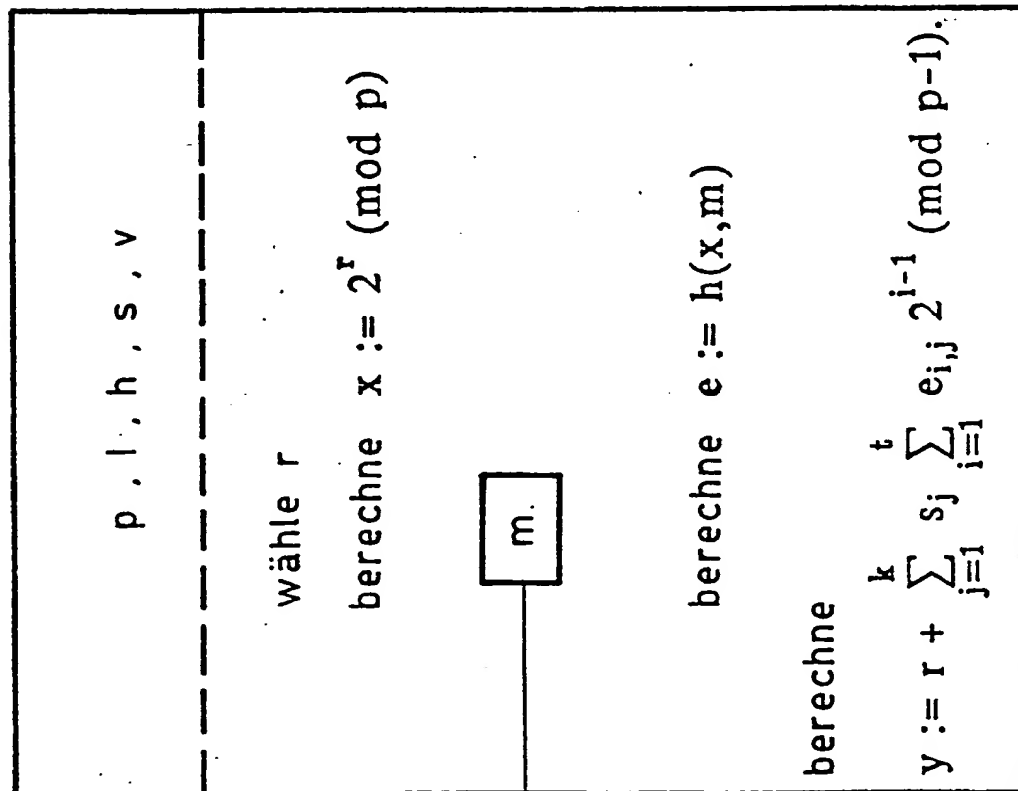
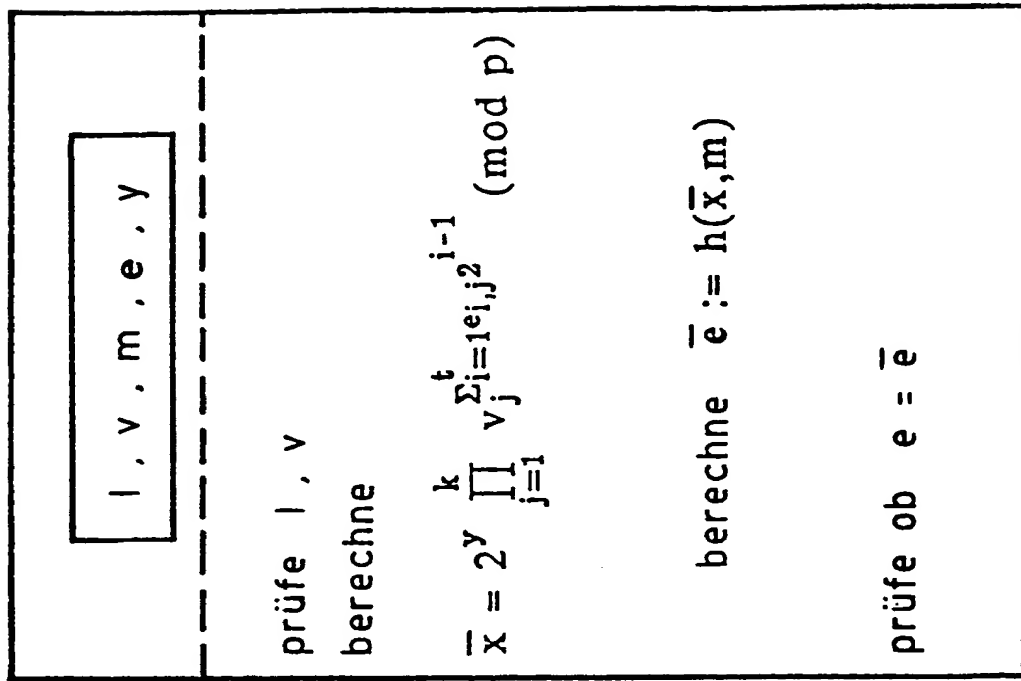


FIG 5

B





Europäisches  
Patentamt

# EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 89 10 3290

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl.5)
A	PROCEEDINGS OF EUROCRYPT '88, Davos, 25. - 27. Mai 1988, Seiten 77-84, Springer-Verlag, Berlin, DE; T. BETH: "Efficient zero-knowledge identification scheme for smart cards" * Seite 78, Zeile 1 - Seite 80, Zeile 2 *	1	H 04 L 9/00
A	IEEE COMMUNICATIONS, Band 25, Nr. 7, Juli 1987, Seiten 73-79, IEEE, New York, US; J.K. OMURA: "A computer dial access system based on public-key techniques" * Seite 75, linke Spalte, Zeile 1 - rechte Spalte, Zeile 20 * -----	1	
			RECHERCHIERTE SACHGEBIETE (Int. Cl.5)
			H 04 L G 07 F
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort DEN HAAG		Abschlußdatum der Recherche 24-10-1989	Prüfer HOLPER G.E.E.
KATEGORIE DER GENANTEN DOKUMENTE X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : mündliche Offenbarung P : Zwischenliteratur		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentedokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus andern Gründen angeführtes Dokument ..... & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	

EPO FORM 1503 03.82 (P0403)

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

